AIRNITE

ZERO DAY

NUMERO 08/2026 · SICUREZZA INFORMATICA

Settimane con le linee ferme: quanto è costato l'attacco informatico a Jaguar Land Rover

A fine agosto 2025 Jaguar Land Rover ha dovuto spegnere i propri sistemi IT dopo un attacco informatico e la produzione è rimasta ferma per settimane. Esperti britannici stimano il danno per l'economia in 1,9 miliardi di sterline. Cosa possono imparare i produttori.

Pubblicato: 21 novembre 2026 Tempo di lettura: 6 min Autore: Redazione Airnite

// LA SITUAZIONE IN CIFRE

£1,9 mld
danno stimato per il Regno Unito
forbice £1,6–2,1 mld, modello del Cyber Monitoring Centre

Categoria 3
"evento sistemico"
sulla scala a cinque livelli del CMC

2.700+
organizzazioni con conseguenze rilevanti
secondo il CMC; altrove ne indica oltre 5.000 coinvolte

08/10/2025
annunciata una ripartenza limitata
secondo il CMC

A fine agosto 2025 Jaguar Land Rover (JLR), il più grande costruttore automobilistico del Regno Unito, ha spento i propri sistemi IT dopo un attacco informatico. Le conseguenze sono andate ben oltre l'azienda: la produzione è rimasta ferma per settimane, i fornitori sono finiti sotto pressione e il governo britannico ha sostenuto JLR con una garanzia sul prestito.

// Cosa è successo?

Secondo la valutazione del **Cyber Monitoring Centre (CMC)**, ente britannico indipendente, del 22 ottobre 2025, l'incidente di fine agosto ha portato allo spegnimento dell'IT e a un lungo stop della produzione. L'**8 ottobre 2025**, sempre secondo il CMC, è stato annunciato il ritorno a una produzione limitata. Stando al CMC, il governo ha concesso una **garanzia su un prestito da 1,5 miliardi di sterline** per fornire liquidità a JLR.

Il CMC classifica l'incidente come **evento sistemico di categoria 3** sulla sua scala a cinque livelli e stima il danno per l'economia britannica in **circa 1,9 miliardi di sterline**, con una forbice tra 1,6 e 2,1 miliardi. Il CMC ritiene possibile che si tratti dell'evento informatico con le conseguenze economiche più pesanti nella storia del Regno Unito. Per l'azienda stessa, BleepingComputer, citando i dati di JLR, ha riportato costi per circa 196 milioni di sterline nel solo trimestre luglio–settembre, esclusi i mancati ricavi.

// Come funziona l'attacco?

Per quanto ci risulta, JLR non ha reso noto nel dettaglio come siano entrati gli aggressori. Il CMC parla di una fuga di dati apparentemente legata all'incidente, senza fornire particolari. Certo è lo schema delle conseguenze: un produttore spegne la propria IT per fermare la propagazione e, poiché la manifattura moderna non funziona senza IT (richiamo dei componenti, pianificazione, controllo, logistica), si fermano anche le linee.

Il modello del CMC tiene conto esplicitamente dei fermi presso JLR, i fornitori e altre aziende della filiera. Non include i costi della fuga di dati né un eventuale riscatto. Il modello ipotizza una ripartenza graduale dall'8 ottobre fino all'inizio di gennaio 2026.

// Chi è colpito?

Non è stata colpita soltanto JLR. Secondo il CMC, **oltre 2.700 organizzazioni britanniche** hanno subito conseguenze finanziarie rilevanti; in un altro passaggio della valutazione si parla di oltre 5.000 organizzazioni coinvolte. Fornitori che non potevano più consegnare i propri componenti, aziende di logistica e concessionari hanno avvertito direttamente il fermo.

Questo rende il caso rilevante per ogni azienda manifatturiera: quanto più produzione, catena di fornitura e IT sono intrecciate, tanto più grande diventa un attacco informatico. E anche chi è ben protetto può restare per settimane senza ordini, se è fornitore di un cliente attaccato.

// Cosa fare adesso?

La domanda centrale è: per quanto tempo riuscite a produrre senza IT, e con quale rapidità tornate operativi? Ne fanno parte una netta separazione tra IT d'ufficio e IT di produzione, backup in grado di sopravvivere a un attacco, piani di ripristino esercitati e una comunicazione di emergenza con fornitori e clienti. La checklist qui sotto riassume i passaggi.

// Come vi aiuta Airnite?

Nella **consulenza** Airnite valuta con voi le dipendenze tra IT e produzione e redige un piano di ripristino. Con **penetration test** verifichiamo se un aggressore potrebbe arrivare dalla rete d'ufficio alla produzione. Con **formazione** ed esercitazioni i vostri team si allenano all'emergenza.

> Nota: i dati sui danni del CMC sono stime basate su un modello. Il dato aziendale di JLR proviene da articoli di stampa; non abbiamo potuto consultare direttamente i comunicati originali di JLR e del governo britannico. Ricerca aggiornata al 21 novembre 2026.

Checklist: cosa fare adesso

[+] Separate a livello di rete l'IT d'ufficio dall'IT di produzione (OT) e controllate rigorosamente i punti di passaggio.

[+] Scrivete piani di ripristino per la produzione ed esercitateli regolarmente, compreso l'ordine in cui i sistemi tornano in funzione.

[+] Impostate i backup in modo che gli aggressori non possano cifrarli insieme al resto (offline o immutabili) e verificate il ripristino.

[+] Coinvolgete fornitori e clienti nella pianificazione delle emergenze: chi viene informato e quando, cosa succede agli ordini in corso?

[+] Calcolate le conseguenze finanziarie di un fermo di diverse settimane e verificate la copertura assicurativa.

[+] Proteggete gli accessi con l'autenticazione a più fattori, in particolare accessi remoti, processi di help desk e account amministrativi.

Come vi aiuta Airnite

- Consulenza – Lo sguardo esterno sui vostri piani e progetti.

- Penetration test e sicurezza – Attacchi controllati con report chiaro e piano di interventi.
- Formazione – Il vostro team impara i nostri strumenti e processi.

Per quanto tempo resterebbe ferma la vostra produzione?

Airnite verifica con voi quanto sono collegate l'IT d'ufficio e la produzione, dove un aggressore potrebbe passare da un ambito all'altro e con quale rapidità ripartireste dopo un incidente. Ricevete misure concrete per separazione delle reti, backup e ripristino.

Richiedete un primo colloquio · Scriveteci un'e-mail · Su WhatsApp

Contatti

Domande su questo articolo? Scriveteci su WhatsApp: +49 174 6834842

Leggi online: https://airnite.de/it/magazine/jaguar-land-rover-attacco-informatico-stop-produzione/

Fonti

Ogni fatto riportato in questo articolo si basa sulle fonti seguenti. Le fonti primarie sono contrassegnate.

1. **Cyber Monitoring Centre · Statement on the Jaguar Land Rover Cyber Incident – October 2025** · 22/10/2025 · FONTE PRIMARIA
   Valutazione indipendente: categoria 3, £1,9 mld di danno (modello), organizzazioni coinvolte, ripartenza, garanzia sul prestito
   https://cybermonitoringcentre.com/2025/10/22/cyber-monitoring-centre-statement-on-the-jaguar-land-rovercyber-incident-october-2025/
2. **BleepingComputer · Jaguar Land Rover cyberattack cost the company over $220 million** · 2025
   Stampa specializzata: costi nel trimestre luglio–settembre secondo i dati di JLR
   https://www.bleepingcomputer.com/news/security/jaguar-land-rover-cyberattack-cost-the-company-over-220-million/
3. **Insurance Journal · Jaguar Land Rover Bailout Shows Rising Cost of Cybercrime** · 07/10/2025
   Stampa economica: sostegno pubblico, inquadramento
   https://www.insurancejournal.com/news/international/2025/10/07/842850.htm

Informazione redazionale di carattere generale, non costituisce consulenza legale né una verifica specifica dei vostri sistemi. Aggiornato alla data di pubblicazione.

Airnite GmbH · Am Waldbach 7 · 77654 Offenburg · airnite.de